DISA

2004 CUSTOMER PARTNERSHIP CONFERENCE

REALIZING THE NET-CENTRIC VISION

Remote Systems Management Through Out of Band Networks

John McCune
GIG Combat Support
Defense Information Systems Agency

REALIZING THE NET-CENTRIC VISION

Trends of Remote Systems Management

- Commercial best practice for systems management evolved to specialized technical support resources and systems management tools at remote locations
- Data centers have become “lights dim” or “lights out”
- Many instances of precedent in government and private sectors

REALIZING THE NET-CENTRIC VISION

Evolution of Computing Services Out of Band (OOB) Management

- Started as a security initiative before transformation to facilitate ports and protocols and “deny by default” access control
- Evolved to a key component of remote systems management as it becomes the transport method for remote event traffic and the access method for privileged access when the access is needed from a remote location

DISA
REALIZING THE NET-CENTRIC VISION

OOB Operational Concept

- Provides capability for managing platforms outside of production connectivity
  - **Closed network to allow out of band access for remote network and infrastructure admin**
  - **Enhanced production security, while maintaining operational access**
  - **Eliminates need to open up firewalls/router ACLs for net management**
  - **Key for remotely managing facilities not for users of applications**

REALIZING THE NET-CENTRIC VISION

CSD OOB Requirements

- Enable administrative access from remote (arbitrary and authorized) locations
- Make ESM logging (event traffic) and monitoring devices unreachable from in-band network
- Encrypt administrative traffic flow from desktop to admin infrastructure
- Authenticate admin access to admin infrastructure
- Eliminate in-band admin access
- Eliminate potential for host-to-host compromise spread through the OOB network
- Standardize access for remote admins (collocated is same as remote)

REALIZING THE NET-CENTRIC VISION

CSD OOB Requirements

- Facilitate secure standup of new platforms that includes process to insure that connection approval criteria have been satisfied
- Support remote access to/by ESM tools for event traffic and automation of host administrative functions
- Create admin access audit trail
- Limit access to host admin by authorization
- Support remote admin of hosts that cannot do host based IDS
- Availability requirements are 7 x 24 x 365

REALIZING THE NET-CENTRIC VISION

Value of Remote OOB Management to Application Owner and Users

- Increased security
- COOP benefits by separating platform from SA
- Ability to give functionals and CDAs authorized privileged access
- More consistent operations when distributed

REALIZING THE NET-CENTRIC VISION

How Application User Can Best Leverage CSD OOB Management

- Be sure platforms have management NICs
- Be sure that platforms can support ESM tools
- Keep application tier separation in application design. Allow for WAN latency between tiers (100 ms rt)
- Assume the application needs to be fielded in a distributed and remotely managed environment

REALIZING THE NET-CENTRIC VISION

Way Ahead

- Remote management of hosts that are not on DISA networks
- At-Large servers
- Separate instance for SIPRNET

REALIZING THE NET-CENTRIC VISION

DEFENSE INFORMATION SYSTEMS AGENCY

BACKUPS

REALIZING THE NET-CENTRIC VISION

Current Design/Implementation

- **Currently designed for 18 operating sites and Issues Center at Hqtrs**
- **WAN Transmission**
  - **Utilize CSD COIN and NIPRNET**
  - **Encryption in WAN for <u>all</u> traffic**
    - **Site to Site VPNs for ESM**
    - **All others will use VPN client for authentication, including co-located workload**

REALIZING THE NET-CENTRIC VISION

Current Design/Implementation

- **VPN Connectivity**
  - **Site to site, to/from ESM suite**
    - **Provides path for production hosts to send/receive ESM traffic**
    - **Each site will have a VPN to both ESM suites**
    - **ESM sites will manage the operations of VPN tunnel and key management**
  - **Client Mode VPNs, SA to Host**
    - **Authorized SA will utilize desktop VPN client to connect to the OOB at the site(s) they administer workload**
    - **Admission criteria require current client key and valid user name/password**
    - **For non-CSD controlled desktops, special VPN client group key created**

REALIZING THE NET-CENTRIC VISION

Current Design/Implementation

- **Authorized uses**
  - **Management protocol traffic (syslog, snmp, Tivoli, Netflow etc.) between hosts and appropriate management or ESM host**
  - **Terminal access from VPN client to host**
  - **Network Time Protocol (NTP)**
  - **DNS for OOB**
  - **Radius or TACACS+ authentication, authorization and accounting**
  - **Any communication between production hosts over OOB is specifically denied. All other communications is denied.**

REALIZING THE NET-CENTRIC VISION

Current Design/Implementation

- **Managed Host Considerations**
  - **Each platform requires dedicated ethernet (10 or 100Mbps) NIC for OOB connectivity**
  - **Host modifications**
    - **Static routes for OOB network to VPN router**
    - **TCP wrappers and other hardening measures applied for management and terminal access for SA**
    - **Terminal access via SSH, unless the platform doesn't have host –based IDS and/or the admin is coming from a Non-CSD controlled desktop**

DISA
REALIZING THE NET-CENTRIC VISION

Current Design/Implementation

- **Access Control**
  - VPN client access is permitted by the client having a group key and a radius authenticated user name/password
  - No unencrypted/unauthenticated packets will traverse the OOB VPN router
  - VLAN ACLs on the OOB layer two switch are “ default-deny”
  - Host level hardening with tools such as TCP wrappers
- **Audit Points**
  - Radius logs of attempted/successful VPN authentication
  - Network based IDS
  - ESM tool suite (HP Openview, Tivoli, Netview, TFMA etc.)
  - Host, switch and router Syslog
  - Host based IDS

REALIZING THE NET-CENTRIC VISION